Web.com is a global internet services company with 3.5 million customers around the world. The company serves primarily small businesses and offers a range of website design and marketing services, including domain hosting, search engine optimization and email – anything a business would need to be visible on the web.

With millions of customers and even more websites under the Web.com umbrella, privacy is crucial to maintain the trust with its small business base. The company has grown through a series of acquisitions and mergers, which has created a diverse matrix of systems and networks that may house personal data.

“We are stewards of our customer’s data,” said Chief Compliance Officer, Peter Heming, who was put in charge of the company’s GDPR efforts. “We don’t own it, it belongs to our customers, and they trust us to protect it.”

Browsing for the perfect GDPR and global privacy partner

Heming began his GDPR efforts in late 2017 and started by reading the letter of the law – literally. He read the GDPR text cover to cover four times before mapping out a plan to tackle the regulation’s demands.

“We don’t view this as a vendor/customer relationship, we see our work with OneTrust as a true partnership.”

Peter Heming
CHIEF COMPLIANCE OFFICER

The Web.com team evaluated a number of vendors and consultants to help with GDPR compliance. Many vendors the team evaluated were either too narrow in their approach, didn’t understand the various nuances of the Web.com business, or couldn’t provide a comprehensive approach to GDPR and global privacy laws, said Heming. After an extensive vetting process, there was a clear frontrunner. “It wasn’t a hard decision to select OneTrust,” said Heming.
The team chose OneTrust because the technology could adapt to the Web.com business as a controller and processor, it was flexible to adjust to various requirements of different global privacy requirements, the platform was intuitive and OneTrust could provide a quick implementation process.

“I've implemented a lot of projects form a vendor and company perspective, and ease of implementation is critical,” said Heming. “We signed with OneTrust in March and were ready to go live prior to the May 25 GDPR deadline. This rapid deployment was critical to our project's success.”

The gateway to a comprehensive privacy program

Web.com leverages a host of OneTrust modules for a comprehensive, global privacy program.

Web.com has multiple consent collection points across its web properties. Heming determined which of their communications – transactions, direct marketing, general marketing, etc. – required consent and which could be considered legitimate interest. He then used OneTrust’s Consent and Preference Management module to manage the various collection points and user preferences.

“OneTrust enabled us to customize consent on storefronts and landing pages,” said Heming.

“OneTrust allows us to understand our data flows, create documentation and generate Article 30 reports for regulators, this is critical for us.”

Peter Heming
CHIEF COMPLIANCE OFFICER

Since Web.com’s affiliate resellers are controllers of data (and Web.com is the processor), affiliates can use OneTrust to submit DSAR requests on behalf of their customers.

“OneTrust’s DSAR portal is effective, easy to use and engaging for our customers,” said Heming.

One of the benefits of using OneTrust for marketing compliance purposes is a complete record and audit trail for consent and subject requests.

In fact, two DSAR requests have been escalated to two separate EU-country DPAs. Heming’s team has used the OneTrust to provide a full audit trail to DPAs that the contested subject requests had been sufficiently fulfilled.

“We had a fully documented audit trail and were able to look back at the request, provide evidence of communications, prove we removed all the data we didn't need to retain of other regulatory purposes. The DPA accepted it and closed the case,” explained Heming.

Web.com also uses OneTrust for assessment automation (PIAs/DPIAs) and data mapping. “OneTrust allows us to understand our data flows, create documentation and generate Article 30 reports for regulators, this is critical for us.”

For assessments, Web.com is able to integrate with JIRA. If a risk is identified in JIRA that’s associated with personal data, it kicks off a simple five-question PIA in OneTrust for a DPO to complete.

Throughout 2019, the Web.com team is looking to automate the privacy program as much as possible. The team is also building out vendor risk and incident and breach lifecycles through the OneTrust platform. Heming’s team is looking to implement the full capabilities through OneTrust’s Vendor Risk Management and Incident & Breach Response modules.

With OneTrust as their partner, Heming believes Web.com can continue to meet regulatory standards and provide excellent experiences for DPOs, employees, partners and customers.

“We don’t view this as a vendor/customer relationship, we see our work with OneTrust as a true partnership,” concluded Heming.